Abstract:

The present invention consists in a system for securing data exchanged between two users having a First Information Processing System (FIPS) and a Second Information Processing System (SIPS) that have been correspondently paired. To complete encryption, the system includes a FIPS to encrypt data with a key, a SIPS to encrypt said key with a stored correspondent key and to encrypt correspondent key identifier with a public key common to the SIPSs. The integrated secured data include FIPS and SIPS encrypted information. The invention is also suitable for decryption. The invention further comprises structures to perform correspondent pairing between two SIPSs in order to exchange secured information. Furthermore, it comprises a pairing method wherein the SIPSs identify each other, exchange ciphered availability codes on the basis of available keys and key identifiers, and also set a correspondence pairing when a key and key identifier available in both SIPSs are identified.